UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/889,410	07/17/2001	J Kitahara	H-996	2813

7590 04/04/2005

John R Mattingly
Mattingly Stanger & Malur
1800 Diagonal Rd
Suite 370
Alexandria, VA 22314

EXAMINER	
SCHUBERT, KEVIN R	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 04/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/889,410	KITAHARA, J	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 February 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-15 have been considered.

Claim Objections

Claim 1 is objected to because of the following informalities: the phrase "internally encrypts sensitive information **encrypted** with said generated key information" should be "internally encrypts sensitive information with said generated key information". The double encryption method is not disclosed in the Specification. The examiner assumes that the applicant meant the phrase to be "internally encrypts sensitive information with said generated key information" and has considered the claim accordingly. Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-2,4-9, and 13-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis, U.S. Patent No. 5,805,712, in view of Yepez, U.S. Patent No. 5,535,168.

As per claim 1, the applicant describes an information processing apparatus comprising the following limitations which are met by Davis in view of Yepez:

a) a processing device for performing predetermined processing of information (Davis: Col 8, lines 2-4);

b) a bus for interconnecting said processing device and other component devices of said information processing apparatus (Davis: Col 8, lines 5-6);

c) wherein said processing device is integrated on a single semiconductor chip, internally generates key information, and internally encrypts sensitive information (encrypted) with said generated key information (Davis: Col 8, lines 7-10; Col 8, lines 20-22);

d) wherein said processing device deletes said key information in said single semiconductor chip if an abnormality is detected (Yepez: Col 1, lines 15-22; Col 4, lines 18-19);

Davis discloses parts a) through c) above as seen by the referenced line numbers and by applicant's admission on the bottom of page 9 of the Remarks, filed 2/28/05. However, Davis does not disclose that key information is deleted in response to an abnormality.

Yepez discloses an apparatus for erasing key information if an abnormality is detected, such as opening the housing containing a device. In Yepez' system, an alarm detector and a memory eraser are part of the information processing apparatus. Adding the alarm detector and memory eraser to the information processing apparatus of Davis would be a simple addition and would provide a more secure information processing apparatus because key information would be deleted in response to a security breach. This means that encrypted information could not be manipulated because the key information is deleted.

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Yepez with those of Davis and add the use of deleting key information because doing so provides more security to the system.

As per claim 2, the applicant describes the information processing apparatus of claim 1, which is anticipated by Davis in view of Yepez (see above), with the following additional limitation which is also anticipated by Davis:

Wherein said control device comprises an external bus controller for preventing non-encrypted sensitive information from being output onto said bus (Col 5, lines 54-67; Col 6, lines 1-7);

The applicant should note the lengthy process which the system goes through in order to ensure that the public/private key pair is unique. Since all the information is sensitive in Davis' system, data is

only output to the bus when it is protected. In a similar fashion, data is only output to the bus in the applicant's system when it is protected.

As per claim 4, the applicant describes the information processing apparatus of claim 1, which is anticipated by Davis in view of Yepez (see above), with the following additional limitation which is also anticipated by Davis:

Wherein a memory device is provided for storing information encrypted by said control device (Col 8, lines 13-17).

As per claim 5, the applicant describes the information processing apparatus of claim 1, which is anticipated by Davis in view of Yepez (see above), with the following additional limitation which is also anticipated by Davis:

Wherein said control device comprises means for decrypting encrypted information at an information write operation (Col 8, lines 13-17);

The applicant should note that the digital certificate at the write operation (storage) comprises means for decrypting encrypted input information.

As per claim 6, the applicant describes the information processing apparatus of claim 5, which is anticipated by Davis in view of Yepez (see above), with the following additional limitation which is also anticipated by Davis:

a) wherein said information processing apparatus is connected to a different information processing apparatus through a network (Col 10, 11-15);

b) wherein said information processing apparatus decrypts encrypted information which is received from said different information processing apparatus (Col 3, lines 27-30).

The applicant should note that the hardware device can transmit information to another device through a network using a transceiver.

As per claim 7, the applicant describes the information processing apparatus of claim 1, which is anticipated by Davis in view of Yepez (see above), with the following additional limitation which is also anticipated by Davis:

Wherein a plurality of said processing devices are provided, and cryptographic processing is carried out in each of said processing devices (Col 6, lines 9-32).

As per claim 8, the applicant describes the information processing apparatus of claim 1, which is anticipated by Davis in view of Yepez (see above), with the following additional limitation which is also anticipated by Davis:

Wherein said processing device comprises means for receiving an encrypted program and for carrying out decryption thereof (Col 6, lines 9-32).

As per claim 9, the applicant describes the information processing apparatus of claim 1, which is met by Davis in view of Yepez (see above), with the following limitations which are met by Davis in view of Yepez:

a) a microprocessor for carrying out said predetermined processing (Davis: 22 of Fig 4);

b) a generator for generating said key information (Davis: 45 of Fig 5; Col 4, line 65);

c) a cryptographic algorithm memory device for storing an algorithm for information cryptographic processing (Davis: 46 of Fig 5; Col 5, lines 11-13);

d) a volatile memory device for storing said generated key information (Davis: 47 of Fig 5; Yepez: Col 7, lines 11-12; Col 2, lines 56-58);

e) a cryptographic processing device for carrying out cryptographic processing with said stored key information according to said algorithm (Davis: 42 of Fig 5; Col 5, lines 1-7);

f) a microprocessor bus for interconnecting said microprocessor, said generator, said cryptographic processing algorithm memory device, said volatile memory device and said cryptographic processing device (Davis: 21 of Figs 4 and 5);

g) wherein a power supply to said volatile memory is stopped so as to delete said key information in said single semiconductor chip if abnormality is detected (Yepez: Col 1, lines 15-22; Col 4, lines 34-36);

The applicant should note that Yepez discloses storing the key information in a volatile RAM memory and deleting the key information if an abnormality is detected. Yepez does not specifically disclose that the key information is deleted by cutting the power supply to the RAM, but he does disclose that "the memory is erased using known erasure techniques" (Col 4, lines 34-35). Cutting the power supply to erase volatile memory such as RAM is a known technique of erasing memory.

As per claim 13, the applicant describes the information processing apparatus of claim 1, which is met by Davis in view of Yepez (see above), with the following limitation which is met by Davis:

Wherein said processing device generates said key information each time sensitive information is encrypted (Davis: Col 5, lines 46-64);

The applicant should note that Davis discloses that a unique device-specific key pair is generated each time sensitive information is encrypted.

As per claim 14, the applicant describes the information processing apparatus of claim 1, which is met by Davis in view of Yepez (see above), with the following limitation which is met by Yepez:

Wherein said abnormality is a disassembly or removal of a case or housing of said processing device (Yepez: Col 4, lines 18-19);

Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Davis in view of Yepez in further view of Hartman, U.S. Patent No. 5,224,166.

As per claim 3, the applicant describes the information processing apparatus of claim 2, which is met by Davis in view of Yepez (see above), with the following additional limitation which is met by Hartman:

Wherein information not requiring encryption is output onto said bus through said external bus controller (Col 3, lines 50-57; Col 6, lines 1-5);

Davis in view of Yepez disclose all the limitations of claim 2. However, Davis' controller method only serves to prevent non-encrypted information from being output onto said bus and Yepez only discloses the method of deleting key data. Thus, Davis in view of Yepez fails to disclose allowing non-encrypted information to be output to the bus.

Hartman describes a bus interface which regulates whether information is output in an encrypted or unencrypted form. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the teachings of Hartman with those of Davis in view of Yepez because it is sometimes necessary for information not requiring encryption to be output to the bus (for example when data is being processed in an already secure area such as the case in Hartman).

Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Davis in view of Yepez in further view of Nagai, U.S. Patent No. 6,571,263.

As per claim 15, the applicant describes the information processing apparatus as described in claim 1, which is met by Davis in view of Yepez (see above), with the following limitation which is met by Nagai:

a) wherein said key information is a random number (Davis: Col 5, lines 3-7);

b) wherein said generator generates said random number based on a signal outputted from a constant voltage diode (Nagai: 8 of Fig 1);

Davis in view of Yepez discloses all the limitations of claim 1. Davis also discloses the use of random number key generation. However, Davis in view of Yepez does not disclose the use of a constant voltage diode in the random number generation.

Nagai discloses a random number generator apparatus which includes the use of a zener diode, which is a constant voltage diode. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Nagai with those of Davis in view of Yepez and add the

use of a constant voltage diode because constant voltage diodes are commonly used in random number generator apparatuses.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 10-12 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

Claim 10 discloses that the disk system controller internally generates key information in response to receiving a request to read out encrypted information. The applicant's specification discloses that upon receipt of a file request the controller reads the encrypted file location information from the disk, decrypts the file location information, reads the encrypted file out of the disk, and transfers the file to the host system (Applicant: page 43). Furthermore, the applicant describes that key information is generated for encryption and retained in the semiconductor device for decryption purposes (Applicant: page 20).

Claim 10 discloses a controller which receives a request for reading out encrypted information and, in turn, internally generates key information. Since key information is only generated when cleartext data is to be encrypted and stored on the disc, the examiner fails to see why key information is generated in response to the controller receiving a request to read out encrypted data. Key information for decrypting the encrypted location of a file may be obtained from storage, but key information is not generated.

Claims 11 and 12 have been rejected as being dependent on claim 10.

Response to Arguments

The applicant's claim for foreign priority and the applicant's amended Abstract as cited in the Remarks, filed 2/28/05, have both been considered and are accepted.

Applicant's arguments with respect to claims 1 and 10 with and the processing device not disclosing deleting key information have been considered but are moot in view of the new ground(s) of rejection.

Applicant's arguments with respect to claim 3 have been fully considered but they are not persuasive. The applicant argues that Hartman does not disclose that the processing device internally generates key information and that Hartman does not disclose deleting key information if an abnormality is detected. While the examiner agrees, the examiner notes that Hartman is combined with Davis in view of Yepez to only add the limitation of a controller outputting information which is not encrypted.

The applicant also argues that Hartman does not disclose that non-encrypted data is output onto the bus by the controller. The controller is the bus interface. As disclosed by Hartman, "Contained within the bus interface is an encryption/decryption module that functions to decrypt incoming encrypted instructions and data on bus for use within CPU chip and to encrypt outgoing data on bus for storage in RAM" (Col 5, lines 37-41). Thus, the bus interface, or controller, outputs both information requiring encryption and information not requiring encryption.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH

shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

***

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER